

## CLAIMS

### WHAT IS CLAIMED IS:

1                   1.     A method, comprising:  
2                   receiving a message;  
3                   selecting a first set of security information from a first plurality of sets of  
4 security information as a function of a property of the message;  
5                   selecting a second set of security information from a second plurality of  
6 sets of security information as a function of the first set; and  
7                   applying the second set of security information to the message.

1                   2.     The method of claim 1, wherein applying the second set of security  
2 information to the message further comprises applying security information derived from  
3 the first set.

1                   3.     The method of claim 1, further comprising determining whether the  
2 message satisfies a security requirement derived from security information of the second  
3 set.

1                   4.     The method of claim 3, wherein determining whether the message  
2 satisfies a security requirement derived from security information of the second set  
3 further comprises determining whether the message satisfies a security requirement  
4 derived from security information of the first set.

1                    5.     The method of claim 3, further comprising rejecting the message if  
2   the message does not satisfy the security requirement.

1                    6.     The method of claim 5, further comprising accepting the message if  
2   the message satisfies all security requirements included in the second set.

1                    7.     The method of claim 6, wherein the message is received after  
2   transmission from a sender.

3                    8.     The method of claim 1, wherein the message is to be transmitted to  
4   another process.

1                    9.     The method of claim 8, further comprising securitizing the message  
2   before the message is transmitted.

1                    10.   The method of claim 1, wherein the second plurality of sets of  
2   security information are shared between nodes of a network.

1                    11.   The method of claim 1, wherein the first set is selected using an  
2   XPath-based expression to match a preselected pattern.

1                    12.   The method of claim 1, wherein the first set is selected using Simple  
2   Object Access Protocol (SOAP) actions.

1                   13.    A machine readable medium having instructions for performing the  
2   method of claim 1.

1                   14.    A method of configuring security scheme of a node in a message-  
2   based system, the method comprising:

3                   loading, in the node, a first plurality of sets of security information related  
4   to security requirements of an application residing in the node;

5                   loading, in the node, a second plurality of sets of security information  
6   related to another set of security requirements; and

7                   loading, in the node, mapping information that maps a set of security  
8   information of the first plurality of sets to a set of security information of the second  
9   plurality of sets.

1                   15.    The method of claim 13, wherein a set of the first plurality of sets  
2   can be selected using an XPath-based expression to match a preselected pattern.

1                   16.    The method of claim 13, wherein a set of the first plurality of sets  
2   can be selected using a predetermined Simple Object Access Protocol (SOAP) action.

1                   17.    The method of claim 13, wherein the second plurality of sets is  
2   shared between nodes of a network

1                   18.    A machine readable medium having instructions for performing the  
2   method of claim 14.

1                   19.    A system comprising:  
2                   a first datastore to include a first plurality of sets of security information  
3   related to an application residing in the system;  
4                   a second datastore to include a second plurality of sets of security  
5   information, wherein a set of the first plurality of sets is associated with a set of the  
6   second plurality of sets; and  
7                   a module to select a first set from the first plurality of sets as a function of a  
8   property of a received message.

1                   20.    The system of claim 19 wherein the first and second datastores are  
2   part of a single larger datastore.

1                   21.    The system of claim 19 wherein the module is further to apply  
2   security information included in a second set of the second plurality of sets to the  
3   received message.

1                   22.    The system of claim 21, wherein the module is further to apply  
2   security information included in the first set to the received message.

1                   23.    The system of claim 21, wherein the module is further to determine  
2   whether the received message satisfies a security requirement included in security  
3   information of the second set

1                   24.    The system of claim 23, wherein the module is further to reject the  
2   message if the message does not satisfy the security requirement.

1                   25.    The system of claim 24, wherein the module is further to accept the  
2   message if the message satisfies all security requirements included in the security  
3   information of the second set.

1                   26.    The system of claim 19, further comprising a third datastore to  
2   include mappings from sets of the first plurality of sets to sets of the second plurality of  
3   sets, wherein the second set is associated with the first set by a mapping included in the  
4   third datastore.

1                   27.    The system of claim 19, wherein the module is to select the first set  
2   using an XPath-based expression to match a preselected pattern.

1                   28.    The system of claim 19, wherein the module is to select the first set  
2   using a predetermined Simple Object Access Protocol (SOAP) action.

1                   29.    The system of claim 19, wherein the second plurality of sets are  
2   shared between nodes of the system.

1                   30. A machine readable medium having components as recited in  
2 claim 19.

1                   31. A machine-readable medium having components, comprising:  
2 means for receiving a message;  
3 means for selecting a first set of security information from a first plurality  
4 of sets of security information as a function of a property of the message;  
5 means for selecting a second set of security information from a second  
6 plurality of sets of security information as a function of the first set; and  
7 means for applying the second set of security information to the message.

1                   32. The machine-readable medium of claim 31, further comprising  
2 means for determining whether the message satisfies a security requirement derived from  
3 the first and/or second sets.

1                   33. The machine-readable medium of claim 32, further comprising  
2 means for rejecting the message if the message does not satisfy the security requirement.

1                   34. The machine-readable medium of claim 32, further comprising  
2 means for accepting the message if the message satisfies all security requirements derived  
3 from the first and second sets.

1                    35.    The machine-readable medium of claim 34, wherein the message is  
2    received after transmission from a sender.

1                    36.    The machine-readable medium of claim 31, wherein the message is  
2    to be transmitted to another process.

1                    37.    The machine-readable medium of claim 36, further comprising  
2    means for securitizing the message before the message is transmitted.

1                    38.    The machine-readable medium of claim 31, wherein the second  
2    plurality of sets of security information are shared between nodes of a network.

1                    39.    The machine-readable medium of claim 31, wherein the means for  
2    selecting the first set uses an XPath-based expression to match a preselected pattern.

1                    40.    The machine-readable medium of claim 31, wherein means for  
2    selecting the first set selects the first set using Simple Object Access Protocol (SOAP)  
3    actions.